I. Sommaire

I. Sommaire 1

II. Introduction générale 2

III. Tripwire 4

A. Introduction 4
B. Pré requis 4
C. Installation du système d'exploitation 4
D. Installation de Tripwire 4
E. Initialisation d'une base de données 5
F. Mise à jour d'une base de données 6
G. Création d'un rapport 7
H. Règles de sécurité 7
I. Fichier de Configuration 8
J. Automatisation 9
K. Utilisation pratique 9
L. Conclusion 10

IV. Prelude 12

A. Introduction 12
B. Fonctionnement de base 12
C. Pré requis 13
D. Installation 14
E. Configuration 15
F. Mise en marche 18
G. Utilisation Pratique 20
H. Un mot sur l'emplacement de la sonde 21
I. Tests effectués 22
J. Conclusion 23

V. Problèmes rencontrés 24

VI. Conclusion générale 26

Annexe 1 28

Annexe 2 30

Annexe 3 37

Annexe 4 38

II. Introduction générale

Ce document décrit la mise en place et l'utilisation du logiciel Tripwire et de la sonde de détection d'intrusion Prelude-IDS (Intrusion Detection System) sur une machine implantée au sein d'un réseau (voir plan en annexe 3). Le but de la sonde est d'observer toutes les anomalies et les tentatives d'attaques, afin d'identifier la source et le but des attaques, pour prendre des mesures préventives et/ou répressives.

En plus du fait qu'ils soient gratuits (sous licence GPL*), leur installation et leur utilisation sont relativement faciles si l'on possède tous les éléments pré requis, ce qui permet l'intégration rapide d'un tel système au sein d'un réseau d'entreprise.

Ils offrent une bonne solution pour des réseaux dont la confidentialité et la sécurité restent relatives, car ce sont des outils "passifs" qui n'agissent pas dynamiquement face à une tentative d'attaque. Ce sont des outils de détection d'intrusion et ils ne sont utiles que si quelqu'un exploite continuellement les fichiers d'audit générés. Sans cela, les logiciels seuls deviennent inutiles.

(*)La licence GPL (GNU General Public License) est une "licence de logiciel libre" : "licence de logiciel" car elle définit un cadre d'utilisation fixé par un programmeur sur son logiciel.
"libre" car le cadre d'utilisation défini par cette licence est - contrairement aux licences classiques - de s'assurer qu'un certain nombre de "libertés" seront respectées sur le logiciel sous licence GPL (ou sur tout logiciel en dérivant). Ces libertés sont les suivantes :
- liberté d'exécuter le logiciel, et ce pour n'importe quel usage ;
- liberté de modifier le logiciel pour l'adapter à ses besoins (dans la pratique, cela nécessite l'accès au code source) ;
- liberté de redistribuer des copies, soit gratuitement, soit contre rémunération ;
- liberté de distribuer des versions modifiées afin que la communauté du logiciel libre puisse en profiter.
(http://www.net-tn.com)

TRIPWIRE

III. Tripwire

A. Introduction

Tripwire est un outil de détection d'intrusion qui permet de vérifier l'intégrité de fichiers, grâce à une prise "d'empreinte" effectuée dès l'installation du système. Cette empreinte est basée sur la taille, la date, et le contenu des fichiers. Il suffit donc de lancer une vérification de ces fichiers au moment où vous le demandez, ou bien, à chaque fois que vous l'avez programmé.

B. Pré requis

Il est important de souligner que l'installation de Tripwire doit se faire sur un système "propre", car il serait inutile de sécuriser un système déjà infecté!

Récupérer les sources de Tripwire (http://www.tripwire.org/downloads/index.php) au format RPM ou tarball.
La version utilisée ici étant *tripwire-2.3-47.bin.tar.gz*

C. Installation du système d'exploitation

Installez le système linux sur une machine non reliée au réseau, pour ne pas être en contact avec une source de pollution potentielle.

D. Installation de Tripwire

Décompresser l'archive, par exemple sous /usr/local/tripwire/, avec la commande :

```
# tar -xzvf tripwire-2.3-47.bin.tar.gz
```

puis installer l'outil:

```
# ./install.sh
```

Après avoir lu la licence, tapez `accept`
confirmer l'installation avec "y".

Le logiciel rappelle qu'un bon mot de passe contient des majuscules et des minuscules, des chiffres, des caractères de ponctuation et d'une longueur de 8 caractères minimum... Pour la manip uniquement, j'utilise des mots simples.

Vous obtenez ensuite les messages suivants:

`Enter the site keyfile passphrase:` entrez une "pass phrase" pour le site, ici ***infanterie***

La pass phrase du site va permettre de créer la clé pour faire une signature des fichiers de config et des règles.

`Enter the local keyfile passphrase:` entrez une "pass phrase" locale, ici ***tripwire***

La pass phrase locale sert pour générer la clé utilisée pour signer la base de données et les rapports.

Après avoir créer les clés, tripwire procède au cryptage et à la signature du fichier de configuration `tw.cfg` :

```
Creating signed configuration file...
```

`Please enter your site passphrase:` rentrez la "pass phrase" du site, ***infanterie***

```
Wrote configuration file: /etc/tripwire/tw.cfg
```

Tripwire écrit donc un fichier de configuration `/etc/tripwire/tw.cfg` dont un exemplaire en format texte est écrit dans `/etc/tripwire/twcfg.txt`. Il est recommandé d'effacer ce fichier texte après l'avoir examiné, car il contient les chemins vers vos fichiers tripwire, dont ceux contenant les mots de passe...

Ensuite processus de cryptage et de signature du fichier de règles `tw.pol`

`Please enter your site passphrase:` rentrez la "pass phrase" du site, ***infanterie***

```
Wrote policy file: /etc/tripwire/tw.pol
```

Comme pour le fichier de config, un exemplaire du fichier `/etc/tripwire/tw.pol` existe en format texte ici : `/etc/tripwire/twpol.txt`

Important:
Ce fichier de configuration, `tw.pol`, est un fichier par défaut, il n'est pas forcement adapté à tous les types de configuration. Vous pouvez choisir votre configuration en éditant le fichier `/etc/tripwire/twpol.txt` (voir plus bas).
Là encore, il est recommander de supprimer ce fichier après l'avoir examiné.

E. Initialisation d'une base de données

La base de données va servir de référence pour la comparaison. Elle contient l'image des fichiers originaux.

Pour l'initialiser, il suffit de tapez la commande:

```
# tripwire –init
```

Le système vous demande alors la pass phrase locale pour crypter le fichier de règles.

Si vous voulez utiliser les fichiers de config par défaut, cela n'est pas déconseillé, mais vous risquez d'avoir des messages d'erreur, car certains fichiers ne sont pas présents sur votre système, en connaissance de cause, il n'est pas nécessaire d'en tenir compte.

Le fichier créer `/var/lib/tripwire/IDS.twd` est l'image de vos fichiers sensibles (IDS étant à remplacer par votre nom de machine). Copiez-le, afin d'en réaliser une sauvegarde.

Vous pouvez créer un checksum de ce fichier avec la commande:

```
# md5sum /var/lib/tripwire/IDS.twd
```

Ce checksum pourra vous aider si par la suite, vous souhaitez vérifier l'intégrité de votre sauvegarde.

F. Mise à jour d'une base de données

Si vous installez ou si vous modifiez volontairement des fichiers de votre base, vous risquez d'avoir des alertes et/ou des erreurs dans les rapports. Pour éviter cela, il suffit de mettre à jour votre base avec:

```
# tripwire --update --twrfile /var/lib/tripwire/report/nomdurapport.twr
```

Cette commande ouvre l'éditeur de texte vi avec votre rapport, en ajoutant le symbole [x] devant les modifications:

```
===============================================================================
Object Summary:
===============================================================================
-------------------------------------------------------------------------------
# Section: Unix File System
-------------------------------------------------------------------------------
Rule Name: Tripwire Data Files (/var/lib/tripwire)
Severity Level: 100
-------------------------------------------------------------------------------
Remove the "x" from the adjacent box to prevent updating the database
with the new values for this object.
Added:
[x] "/var/lib/tripwire/IDS.twd"
-------------------------------------------------------------------------------
Rule Name: Root config files (/root)
Severity Level: 100
-------------------------------------------------------------------------------
Remove the "x" from the adjacent box to prevent updating the database
with the new values for this object.

Modified:
[x] "/root/.kde/share/config"
[x] "/root/.kde/share/config/konquerorrc"
```

Laissez les marques devant les fichiers que vous voulez ajouter à la base.
Sortez de l'éditeur avec la commande (Esc) :wq
Vous devez entrer la pass phrase locale pour enregistrer les modifications.

G. Création d'un rapport *(voir annexe 1)*

La création d'un rapport se fait avec la commande:

```
# tripwire --check
```

Le rapport créé dans `/var/lib/tripwire/` et sous la forme:
`nomdemachine-date-heure``.twr`, la date et l'heure sont celles de la génération du rapport.

On peut voir les modifications dans la partie "Rule Summary", une * marque les règles ayant fait état d'un changement (ajout, suppression ou modification).

Puis, dans la partie "Object Summary", on voit le détail des fichiers signalés.

Les rapports générés sont cryptés, pour les visualiser il faut donc taper la commande:

```
# twprint -m r -r  /var/lib/tripwire/report/nomdurapport.twr
```

H. Règles de sécurité

Le fichier `/etc/tripwire/tw.pol` contient les règles de sécurité à appliquer. Ce fichier est crypté. Il est possible de recréer ce fichier au format txt avec la commande suivante:

```
# twadmin --create-polfile -S site.key /etc/tripwire/twpol.txt
```

Vous devrez entrer la pass phrase du site.

Sous cette forme vous pourrez alors le modifier pour l'adapter à votre configuration.

Voici quelques paramètres utiles :

`/etc/passwd -> +pingus;`	Vérifier le fichier passwd selon les attributs p, i, n, g, u, et s.
`!/etc/passwd/;`	Ne pas (!) vérifier le fichier passwd.
`/etc -> +ug (recurse=false);`	Vérifier /etc mais pas le contenu
`/etc -> +ug (emailto=admin@domain.com);`	Envoi un email à l'adresse indiquée si l'user ou le groupe est modifié

Quelques attributs:

```
/etc/passwd -> +g;        # File owner's group ID
/etc/passwd -> +i;        # Inode number
/etc/passwd -> +m;        # Modification timestamp
/etc/passwd -> +p;        # Permissions and file mode bits
/etc/passwd -> +r;        # Device Number
/etc/passwd -> +s;        # File size
/etc/passwd -> +t;        # File Type
/etc/passwd -> +u;        # File owner's user ID
/etc/passwd -> +l;        # File is increasing in size
/etc/passwd -> +C;        # CRC-32 hash value
/etc/passwd -> +M;        # MD5 hash value
```

Dans le fichier par défaut, certaines variables sont prédéfinies:

```
$(IgnoreAll);ignore les attributs p,i,n,u,s,g,l,a,m,c,t,d,b,C,M,S,H
$(IgnoreNone);      équivaut aux attributs +pinusgamctdbCMSH
$(Dynamic);         équivaut aux attributs +pinugtd
...


SEC_CRIT = $(IgnoreNone)-SHa ;   Fichiers critiques qui ne peuvent pas changer
SEC_SUID = $(IgnoreNone)-SHa ;   Binaire avec le bit SUID ou SGID positionné
SEC_BIN  = $(ReadOnly) ;         Binaire qui ne doit pas changer
SEC_CONFIG = $(Dynamic) ;        Fichier de config qui change peu mais d'accès
                                 fréquent
SEC_LOG = $(Growing) ;           Fichier changeant mais de propriétaire fixe
SEC_INVARIANT = +tpug ;          Répertoire ne changeant pas de permission ni de
                                 propriétaire
SIG_LOW       = 33 ;             Fichier non critique avec un niveau de
                                 sécurité faible
SIG_MED       = 66 ;             Fichier non critique avec un niveau de sécurité
                                 important
SIG_HI        = 100 ;            Fichier vulnérable avec un niveau de sécurité très
                                 important
```

Tous les paramètres sont disponibles dans le fichier `/usr/doc/tripwire/policyguide.txt`.

Une fois les modifications appliquées au fichier de règles, il faut réinitialiser la base de données avec la commande :

```
# tripwire --init
```

Pensez à effacer ensuite le fichier .txt !!!

I. Fichier de Configuration

Le fichier de configuration `tw.cfg` contient, entre autres, les paramètres suivants:

localisation du répertoire root de tripwire,
localisation du répertoire de règles de sécurité,
localisation du répertoire de la BdD,
localisation du répertoire des rapports,
localisation du répertoire des clés,
localisation du répertoire de l'editeur de texte (vi),
...

Pour « sécuriser » un peu plus l'application Tripwire, il est conseillé de modifier les chemins par défaut de ces fichiers.

Le fichier `tw.cfg` est, là encore, un fichier crypté. Pour recréer un équivalent en format texte, il suffit de lancer:

```
# twadmin --create-cfgfile -S site.key /etc/tripwire/twcfg.txt
```

Il suffit alors de modifier le fichier `/etc/tripwire/twcfg.txt`, puis de relancer une initialisation de la base de données.

Pensez à effacer ensuite le fichier .txt !!!

J. Automatisation

Par email

Il est possible d'envoyer un email quand un rapport est effectué, en ajoutant la ligne "`emailto = login@nomdedomaine`" dans le fichier `twpol.txt`. Ce processus se fait par sendmail par défaut, mais peut être configuré par le fichier `twcfg.txt` à la ligne `MAILMETHOD`.

Cela donne, pour l'envoi par email :

```
(
rulename = "Networking Programs",
severity = $(SIG_HI),
emailto = login@nomdedomaine
)
```

Par crontab

La fonction crontab du système linux, apporte une fonction complémentaire qui permet par exemple, de lancer la vérification automatiquement, à une fréquence donnée.
Par exemple pour faire une vérification chaque jour et recevoir un email avec le contenu du rapport il suffit de rajouter un script dans le répertoire `/etc/cron.daily/` :

le script pourrait être le suivant:

```
#!bin/bash
HOST_NAME=`uname -n`
if [ ! -e /var/lib/tripwire/${HOST_NAME}.twd] ;
then
      echo "*** Erreur: Base de donnée pour ${HOST_NAME} non trouvée. ***"
      echo "*** Executez: "/etc/tripwire/install.sh" et/ou "tripwire --init". ***"
else
      test -f /etc/tripwire/tw.cfg && /usr/sbin/tripwire --check
fi
```

Ce fichier vérifie l'existence d'une base de donnée tripwire, si elle est présente, il exécute la fonction tripwire –check, sinon il génère un message d'erreur

K. Utilisation pratique

En fait, sous un système UNIX, l'utilisation des répertoires nous facilite un peu le travail, car chacun de ces répertoires regroupe souvent, un ensemble de commandes bien définies.

Il convient donc de spécifier dans le fichier `tw.pol`, les fichiers se trouvant sous :

/bin contenant l'ensemble des commandes de base communes à tous les utilisateurs et donc les fichiers absolument invariables.
/sbin contenant les commandes système. Là encore des fichiers absolument invariables.
/dev fichiers spéciaux relatifs aux périphériques.
/etc commande de maintenance et configuration système.

Ensuite on peut y ajouter :

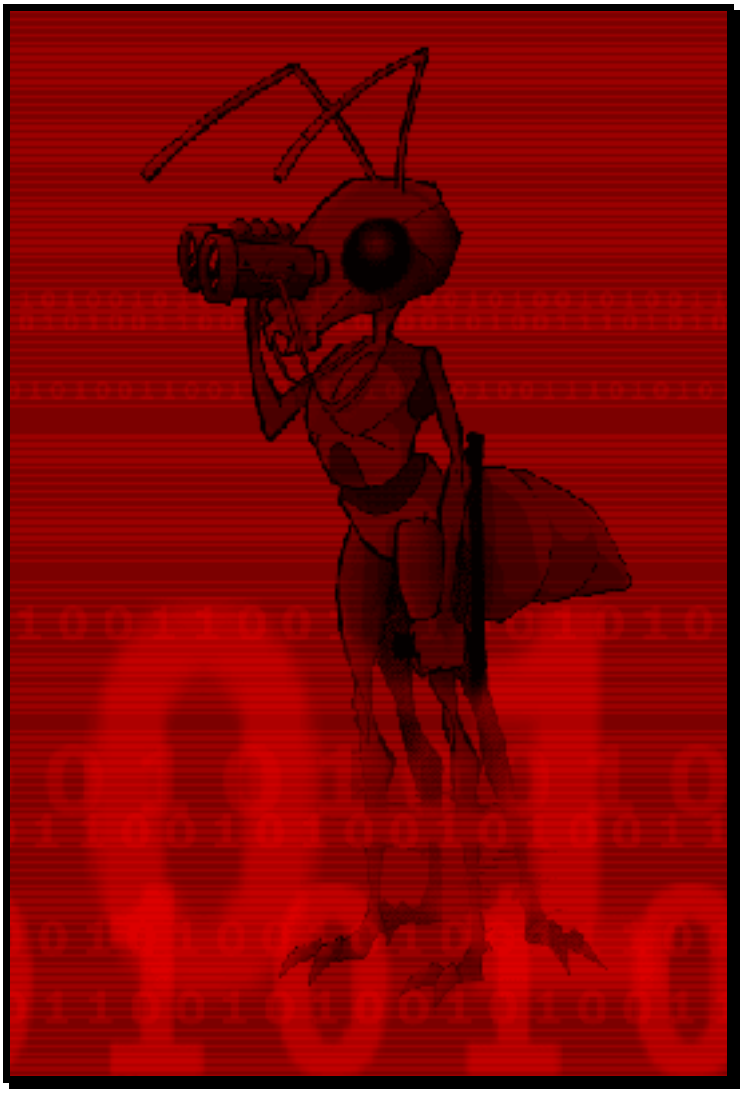
/lib les librairies de base.
/var fichiers systèmes variables, fichiers de log.
/usr/bin commandes utilisateur supplémentaires.
/usr/sbin commandes système supplémentaires.

Attention à positionner les attributs sur un fichier en fonction de ses propriétés, car le rapport de vérification risquerait de contenir des avertissements inutiles, si par exemple vous choisissez un attribut de vérification sur la taille à un fichier de log…

L. Conclusion

Tripwire constitue un des premiers éléments de protection passive pour une station ou un serveur. Il n'est qu'une petite partie d'un processus de sécurisation, et doit être utilisé avec d'autres logiciels permettant de mettre en oeuvre une protection plus importante des login/password utilisateur (logiciel npasswd,...), mise en place d'un Firewall, etc...

Sa mise en place et son fonctionnement sont simples, et son mode de fonctionnement de type une règle par fichier, permet de cibler exactement les besoins. Sa configuration s'adresse à des utilisateurs ayant connaissance des principes de fonctionnement d'un système UNIX, au moins pour le choix des règles de sécurité.



PRELUDE

IV. Prelude

A. Introduction

A l'origine, le but du projet Prelude était de créer un outil modulaire de détection d'intrusion. Puis de nouvelles recherches ont transformé la sonde d'intrusion réseau (NIDS) en projet Hybride, portant à la fois sur une sonde réseau et une sonde locale « host based ». Aujourd'hui, Prelude-IDS est devenu un outil modulaire, distribué, robuste et rapide, tout en gardant son aspect « hybride » Local / Réseau.

Son fonctionnement s'appuie sur la comparaison de trames circulant sur un réseau, avec une base de signatures de tentatives d'intrusions et d'autres anomalies. Ces signatures sont basée sur celles d'un autre projet d'IDS : S.N.O.R.T.

Chaque trame anormale est stockée avec tous ses renseignements, dans un fichier de logs, et dans une base de donnée SQL.

Un module additionnel permet de gérer cette base SQL, grâce à une interface web. Pour le détail du fonctionnement de Prelude, je vous renvoi au document de Guillaume Arcas et au magazine M.I.S.C. *(voir ressources en annexe 4)*.

Bien que le but du projet Prelude soit une architecture distribuée, pour le mini projet, tous les modules ont été installés sur la même machine. L'esprit, la fonctionnalité et la technique restant les mêmes.

B. Fonctionnement de base

La sonde se compose de 4 modules principaux + 1 interface web :

Libprelude :	Elément de base de tous les modules, elle contient toutes les fonctionnalités. C'est elle qui assure la communication entre les capteurs et le manager. Elle permet de négocier si la connexion peut s'établir en SSL *(clés publiques + certificats)*.
Prelude-manager :	C'est l'élément qui reçoit les messages des capteurs et les transforme en alertes. Ces alertes sont ensuite stockées dans une base de données SQL, pour être exploitées ensuite par l'interface web frontend.
Prelude-NIDS :	C'est l'élément qui permet la capture de trames en temps réel. Il se base sur une version de la librairie pcap. Il est capable de décoder des requêtes HTTP, FTP et TELNET, d'analyser des trames en fonction des signatures SNORT, de détecter les scans, ArpSpoof (Arp en Unicast), et d'autres encore…
Prelude-LML :	Il peut servir a recueillir les logs de diverses plates-formes, comme des machines Unix, Firewalls, etc… Installer en local, il permet d'analyser des fichiers de log locaux, afin de vérifier les accès par login, par exemple.

Frontend : C'est l'interface web d'administration de la sonde. Il existe plusieurs types d'interfaces : en Php (abandonnée) et une en Perl (offre plus de possibilités).

Prelude fonctionne de la manière suivante :

Les capteurs NIDS, placés soit en local, soit dispersés sur des machines du réseau, capturent les trames douteuses, analysent leur contenu et s'il y a anomalie, envoie une alerte contenant les informations de la trame incriminées au manager.

Les capteurs LML, locaux ou distribués, vérifies les fichiers de log afin de déceler, là encore, toute anomalie. Si quelque chose est détecté, les capteurs communique au manager les infos en questions.

Le manager traite ces alertes en remplissant des tables dans une base de données, en fonction du type, des adresses, du contenu, et de toutes autres infos importantes. L'interface permet d'afficher les alertes contenues dans la base, de manière conviviale, en proposant quelques fonctions de base : Lister, effacer, utilisation de filtres, statistiques,…

C. Pré requis

Un système d'exploitation Linux, avec un serveur web, et un serveur SQL

Ici Debian 3.0r0, choisi pour la facilité d'utilisation, surtout au niveau des packages, où les dépendances s'installent automatiquement avec la commande apt-get...
Serveur web Apache 1.3.26-0woody3, et serveur SQL MySQL 3.23.49-8.4.

Librairies à installer pour la sonde :

libssl-dev	pour permettre l'accès sécurisé, nécessaire à libprelude, prelude-manager, et prelude-nids/lml
mysql-server	pour le serveur de base de donnée
libmysqlclient10-dev	pour le client mysql, pour prelude-manager
libpcre3	librairie perl pour prelude-lml
libfam	pour prelude-lml

Librairie à installer pour le manager Piwi :

Apache-ssl	serveur web avec prise en charge SSL.
libdbi-perl	librairie nécessaire pour l'accès à MySQL
libgd-graph-perl	librairie graphique pour perl
libgd-graph3d-perl	librairie 3D pour perl
libdate-calc-perl	interface perl pour le calendrier.
Geo::IP	interface de localisation d'adresse IP

Modules Prelude utilisés:

libprelude-0.8.5
prelude-manager-0.8.7
prelude-nids-0.8.1 (NIDS = Network IDS)
prelude-lml-0.8.3 (LML = Log Monitoring Lackey encore appelée HIDS, Host IDS)
Piwi ou frontend-perl (P(erl|relude) IDS Web Interface)

Les modules sont disponibles sur le site Prelude : http://www.prelude-ids.org/
Les anciennes versions sont disponibles sur : http://www.prelude-ids.org/download/
Le module piwi est disponible sur : http://www.leroutier.net/Projects/

D. Installation

L'installation des modules se fait en décompressant les archives tar :

```
# tar ?xzvf nomdumodule.tar.gz
```

Module libprelude

Le module libprelude est la base du logiciel. Il doit être installé en « binôme » avec le manager, le capteur NIDS et le capteur Local, car ces trois derniers puisent leurs fonctions dans ce module :

Exemple d'installation en architecture distribuée :
Sur la machine Alpha, sonde réseau, j'installe libprelude et prelude-nids
Sur la machine Bravo, sonde locale, j'installe libprelude et prelude-lml
Sur la machine Charlie, station de management, j'installe libprelude, le manager et frontend.

Sur la machine locale :
Les modules librelude, le manager un ou les deux capteurs, et le frontend.

L'installation se fait à partir du répertoire décompressé :

(Pour les options de configuration passez la commande: `./configure --help`)

```
# ./configure --enable-openssl
```
installe la librairie avec prise en charge du module SSL
```
# make
# make install
```

Le SSL permet aux sondes dispersées à travers le réseau, de communiquer au moyen d'un protocole d'authentification.

Les clés et le certificat se trouvent dans `/usr/local/etc/prelude-sensor/`.

Module prelude-manager

Pour son installation, on lui rajoute l'option de prise en charge de base de données MySQL, car cette base sert pour le gestion d'alertes par l'interface web.

```
# ./configure --enable-mysql --enable-openssl
# make
# make install
```

On peut noter que la base PostgreSQL peut aussi être utilisée, en remplaçant l'option par :
`--enable-postgresql`

Module réseau prelude-nids

On continue, toujours

```
# ./configure
# make
# make install
```

Module local prelude-lml

Et enfin, on rajoute l'option FAM (File Alteration Monitor) qui permet au capteur local de gérer le changement de propriétés d'un fichier.

```
# ./configure --enable-fam
# make
# make install
```

Module de management piwi

Une fois décompressé, il faut installer le module à la racine de votre site web.
Sur apache: /var/www/piwi/, par exemple.

E. Configuration

Configuration Mysql

Il faut lancer le serveur mysql :

```
# /etc/init.d/mysql start
```

Puis créer la base de données Prelude :

```
# mysql
mysql> create database prelude ;
quit
```

Il faut maintenant changer les propriétés du script qui va créer les tables dans la base. On lui attribut ces propriétés pour qu'il soit exécutable par root :

```
chmod 550 /usr/local/bin/prelude-manager/prelude-manager-db-create.sh
```

puis lancer le script :

```
# /usr/local/bin/prelude-manager-db-create.sh
```

Répondre aux étapes suivantes :

```
0/7 -> y
1/7 -> mysql
2/7 -> localhost
3/7 -> 3306
4/7 -> prelude
5/7 -> root   attention ne pas entrer de mot de passe !!
6/7 -> perlude  mot de passe : 1ri2ch
7/7 -> yes
```

Configuration du manager

Dans le fichier :

```
/usr/local/etc/prelude-manager/prelude-manager.conf
```

Décommenter et renseigner les lignes suivantes :

```
sensors-srvr = 192.168.1.20
```
pour l'adresse d'écoute des sondes

```
[MySQL]

# Host the database is listening on.
dbhost = localhost;
# Name of the database.
dbname = prelude;
# Username to be used to connect the database.
dbuser = prelude;
# Password used to connect the database.
dbpass = 1ri2ch;
```

Configuration nids

Dans le fichier :

```
/usr/local/etc/prelude-nids/prelude-nids.conf
```

Décommenter et renseigner :

```
manager-addr = 192.168.1.20 ;
```
adresse du manager

```
user = prelude ;
```
utilisateur de la base

Configuration lml

Dans le fichier :

```
/usr/local/etc/prelude-nids/prelude-nids.conf
```

Décommenter et renseigner :

```
manager-addr = 192.168.1.20 ;          adresse du manager
```

Configuration du module Piwi

Dans le fichier httpd.conf on trouve le profil d'utilisateur d'apache :
Sous debian :

```
User www-data
Group www-data
```

Pour que le serveur puisse accéder aux fichiers et exécuter les requêtes, il faut donner aux fichiers et au répertoire piwi, les accès nécessaires :

```
chown –R www-data.www-data /var/www/piwi/
chmod –R u+x /var/www/piwi/
```

Prise en charge de MySQL

Dans le fichier `/var/www/piwi/Functions/config.pl`

Renseigner les lignes suivantes :

```
$conf{'dbtype'}='mysql' ;                          type de la base de données
$conf{'dbname'}='prelude' ;                        Nom de la base
$conf{'dbhost'}='localhost' ;                      Nom de la m achine hôte
$conf{'dbport'}='3306' ; # default mysql port is 3306
$conf{'dblogin'}='prelude' ;                       Login user de la Base de données
$conf{'dbpasswd'}='1ri2ch' ;                       Pass user de la base
```

Modification dans le fichier de configuration d'apache /etc/apache/httpd.conf

Pour que le serveur prenne en charge le langage perl, il faut modifier son fichier de configuration :

```
Listen 192.168.1.20
DirectoryIndex index.pl index.html index.thm
ServerName localhost
DocumentRoot /var/www/
```

Puis modifier les lignes suivantes:

```
# If the perl module is installed, this will be enabled.
<IfModule mod_perl.c>
  Alias /perl /var/www/perl/
    <Location /perl>
       SetHandler perl-script
       PerlHandler Apache::Registry
```

```
      Options +ExecCGI
    </Location>
</IfModule>
```

en:

```
# If the perl module is installed, this will be enabled.
<IfModule mod_perl.c>
  Alias /perl /var/www/piwi/
    <Location /var/www/piwi>
       SetHandler perl-script
       PerlHandler Apache::Registry
       Options +ExecCGI
    </Location>
</IfModule>
```

Puis après les lignes :

```
# PerlModule Apache DBI
# …
# …
# …
```

Ajouter :

```
<Directory "/var/www/piwi/">
  Options ExecCGI
  AddHandler cgi-script .pl
</Directory>
```

Note :

Une fois tout installé, il est possible de tester la mise en place de l'interface perl en allant sur l'url :
http://192.168.1.20/piwi/test/test.pl

Les modules apparaissant en vert sont fonctionnels, ceux en rouge sont absents.

F. Mise en marche

Enregistrement des capteurs dans prelude-manager :

Afin d'enregistrer un capteur auprès du manager, il faut passer par une procédure d'authentification. On commence par lancer la procédure du coté manager, il donne un mot de passe servant à l'authentification et il se met en attente d'un capteur :

```
# manager-adduser
```
retenez le mot de passe qui vous est donné.

Enregistrement de la sonde réseau :

Ensuite, il faut lancer l'enregistrement du côté du capteur :

```
# sensor-adduser –s prelude-nids –m 192.168.1.20 –u 0
```

-s pour le nom du capteur
-m pour l'adresse du manager
-u pour l'uid utilisé par le capteur (root)

(pour les autres options tapez sensor-adduser --help)

Entrez le mot de passe fourni à l'étape précédente. Puis entrer le nom d'user et le pass de la base SQL : user *prelude*, pass *1ri2ch*

Enregistrement de la sonde locale :

Lancement de l'enregistrement du capteur local :

```
# sensor-adduser –s perlude-lml –m 192.168.1.20 –u 0
```

-s pour le nom du capteur
-m pour l'adresse du manager
-u pour l'uid utilisé par le capteur (root)
(pour les autres options tapez sensor-adduser --help)

Entrez le mot de passe fourni à l'étape précédente. Puis entrer le nom d'user et le pass de la base SQL : user *prelude*, pass *1ri2ch*

Lancement de l'écoute sur le manager :

Une fois tous les capteurs enregistrés on lance l'écoute du manager :

```
# prelude-manager
```

ou sans avoir renseigné le fichier de configuration :

```
# prelude-manager --mysql –-dbhost localhost –-dbname perlude –-dbuser prelude –-
dbpass 1ri2ch
```

Lancement de la sonde réseau

```
# prelude-nids –i eth0 –u root
```

Cette commande démarre l'écoute des trames, et donc l'envoi de messages d'alertes si une anomalie est détectée.

Lancement de la sonde lml

```
# prelude-lml –i eth0 –u root
```

Cette commande démarre la surveillance des fichiers de log.

Lancement du module piwi

Sur votre navigateur web tapez l'url:

http://192.168.1.20/piwi/Filters.pl

Vous avez alors accès au module de management web en tant que « guest ».

Vous pourrez uniquement avoir le rôle de « spectateur ».

Pour avoir la possibilité d'effacer les logs il faut modifier les droits de guest dans le fichier `/var/www/piwi/Profiles/guest.user`
Et remplacer les valeurs *none* par ***`all.`***

Il est possible de supprimer ce fichier `guest.user` et de renommer le fichier `admin.user` en `guest.user .`

G. Utilisation Pratique

L'utilisation da la sonde en elle-même se limite au choix des règles de filtrages et à la mise en marche des capteurs NIDS et LML.

La partie la plus importante reste dans l'utilisation l'interface web.
Elle est très intuitive, il suffit de suivre les liens. Je ne m'étendrais pas dans une explication rubrique par rubrique, je laisse en annexe 2 des captures d'écran, qui parlent d'elles mêmes.

L'utilité et l'utilisation principales restent dans l'exploitation des alertes et à la mise en place de parades. La difficulté est donc de s'imprégner de la documentation, de se tenir à jour sur les types d'attaques et les parades. Dans ce domaine, la veille technologique est très importante car les attaques évoluent aussi rapidement que la technique.

Note :
Sylvain Loeuillet, qui a contribué à la réalisation du module frontend-perl, met à votre disposition une interface de démonstration, sur l'url suivante :
http://www.leroutier.net/Projects/PreludeIDS/Demo/Filters.pl

Localisation des fichiers utiles

Prelude manager

Fichier de config :
`/usr/local/etc/prelude-manager/prelude-manager.conf`

Prelude nids

Fichier de config :
`/usr/local/etc/prelude-nids/prelude-nids.conf`

Répertoire des règles de filtrages:
`/usr/local/etc/prelude-nids/ruleset/`

Prelude lml

Fichier de config :
`/usr/local/etc/prelude-lml/prelude-lml.conf`

Répertoire des règles de filtrages:
`/usr/local/etc/prelude-lml/ruleset`

Fichiers d'alertes:

```
/var/log/perlude.log
/var/log/mysql.log        requetes SQL effectuées
```

Script permettant de convertir les règles SNORT pour Prelude
http://www.prelude-ids.org/download/contribs/convert_ruleset

Prelude-perl-frontend

Fichiers de documentation :
/piwi/Docs/

Fichiers de test :
/piwi/test/

Important

Prelude est lui aussi soumise à des attaques, notamment de types DoS, IP Soofing,…
Elle est d'ailleurs vulnérable et il existe un patch pour éviter l'IP Spoofing.

Ce patch se trouve ici :
http://sylvain.detilly.free.fr/ids/download/prelude-nids--address-spoof-plugin.patch

La librairie libsafe peut être rajoutée pour protéger un processus des vulnérabilités sur les débordements de tampon. Si une tentative de débordement est détecté, il envoi une alerte à la sonde.

Je ne l'ai pas testé pas manque de temps…

H. Un mot sur l'emplacement de la sonde

Il est important de placer les sondes réseau et les sondes locales à des endroits stratégiques.
Pour le mini projet, la localisation par rapport au réseau global (en annexe 3), peut s'expliquer de la sorte :

- La sonde réseau est placée sur le segment faisant la jonction entre le réseau « local » et le réseau « externe » afin de surveiller le trafic global entrant et sortant.
- Elle se place aussi entre l'extérieur (source potentiellement dangereuse) et les serveurs Web et FTP (victimes potentiellement vulnérables), car on peut estimer qu'il faut accroître la surveillance à ce niveau précis.

L'installation de capteurs NIDS ou LML, entre autre, au niveau des firewalls Astaro et Censornet, aurait pu venir compléter la surveillance. Ces firewalls basés sur une architecture UNIX, auraient sans doute accepté l'installation de ce type de capteur.

I. Tests effectués

Sur le capteur NIDS

Une fois les outils installés, j'ai effectué 2 tests simples afin de vérifier les réactions de la sonde.

Disposant d'un serveur WEB, FTP dans la DMZ du firewall CHECKPOINT, ce serveur offrait une cible potentielle.

Pour ces tests, je me suis placé sur une station hors du réseau du mini projet. Cette station avait pour adresse 192.168.24.84/24.

1er test :

Tentative d'attaque en utilisant la faille « Microsoft IIS Unicode Exploit », exploitable lorsque le site web garde ces paramètres par défaut (notamment les fichiers et répertoires)

Sur le navigateur de la station test j'entre l'url suivante :
http://172.16.19.10/scripts/..%c0%af../winnt/system32/cmd.exe?/c+dir+c:\
qui va tenter de lister le contenu du disque du serveur sur mon navigateur.

La sonde a détecté la trame contenant l'url et remonte une alerte « WEB IIS cmd.exe acces ».

L'attaque a échoué car le serveur a supprimé les répertoires par défaut.

2ème test :

Utilisation d'un scanner de port (Superscan).
Toujours à partir de la station test, je lance un scan sur l'adresse du serveur (172.16.16.10/26) en testant les numéros de ports ouverts entre 1 et 1024.

J'obtiens une liste de port sur le scanner, dont les ports 80 et 21.

La sonde prelude a bien détecté le scan et remonte une alerte « ICMP Superscan ».

Une parade possible est de coupé les trames ICMP à partir du firewall.

Sur le capteur HIDS

Je n'ai pas approfondi l'utilisation du capteur local pour plusieurs raisons :

- manque de connaissances et de moyens d'attaques nécessaires, pour tester l'efficacité des règles de sécurité appliquée aux fichiers de logs.
- manque de temps.
- la sonde Tripwire étant installée, je me suis appuyé sur ces rapports pour la sécurité locale, malgré le fait qu'elle ne se base pas sur les mêmes principes de règles.

En revanche, j'ai pu remarquer que la sonde se basait sur les fichiers de log :
`var/log/messages`, et `/var/log/auth.log` pour le niveau local, lui permettant de connaître

chaque identité qui loguée sur la machine et si ces connexions ont réussi ou échoué. Ce que ne permet pas directement Tripwire.

J. Conclusion

Prelude est une bonne approche concernant l'adoption d'une solution de sécurité. Comparé à du matériel dédié, lorsque les performances sont proches, ce projet peut mettre en avant sa licence GPL qui reste à mon sens, un de ces plus gros atouts face à l'utilisation d'un tel moyen en entreprise. Le fait que ces capteurs HIDS surveillent également d'autres types de fichiers de logs, peut apparaître là aussi comme un avantage.

Son point faible restant dans l'utilisation de « contre-mesures », qui est encore à l'état de projet. On pourrait attendre une amélioration de l'interactivité avec l'utilisateur et/ou d'autres logiciels/matériels, en apportant des remontées d'alertes importantes instantanées à la manière des « trap » SNMP, afin d'agir directement sur un firewall, un switch,… Mais je pense que ce n'est qu'une question de patience, car le projet Prelude, et en constante évolution.

V. Problèmes rencontrés

Pour Tripwire :

Pas de difficultés majeures.

La remarque la plus importante reste qu'il faut modifier le fichier de config tw.pol pour ne pas avoir de messages d'erreur. En effet, par défaut, ce fichier contient des répertoires et des fichiers qui ne se trouve pas sur votre système. Quand tripwire lance une initialisation ou une vérification, il ne les trouve pas et génère des erreurs dans le rapport. Ces erreurs ne sont pas importantes, mais « polluent » inutilement le rapport.

Il a fallu faire un choix sur les fichiers systèmes à auditer et sur quelles règles. Ce travail est assez long mais il est nécessaire si l'on veut être efficace.

Pour Prelude :

Ma configuration de départ était une version RedHat 7.2 Advanced Server, avec serveur Web Apache, et serveur MySQL.

Les modules de Prelude étant ceux décrits dans la manip.

J'ai opté pour une interface web en php (prelude-frontend-php), car elle était souvent décrite dans les archives trouvées.

Déroulement du test :

L'installation du logiciel en lui-même ne pose pas de problème, le lancement de la sonde se fait correctement, et j'obtiens un fichier de log comportant les alertes `(/var/log/prelude.log)`.

Le fichier de log grossissant à vu d'œil, je décide de couper la sonde et d'installer le module frontend-php, qui permet d'accéder à la base de données contenant les alertes. Ce module permet d'avoir une interface graphique plus conviviale des fichiers de log.

Là encore l'installation de l'interface se fait conformément aux documents récupérés (cité en annexe 4).

1er problème :
Monter un serveur web avec prise en charge de php4 et MySQL, qui fonctionne !
N'ayant pas installé les modules nécessaires dès l'installation du système, j'ai du monter ces modules manuellement. Après plusieurs essais, j'ai eu des problèmes de dépendance entre ces 3 modules et les trois services ne fonctionnaient pas correctement.

Résolution :
J'ai donc réinstallé le système en incluant dès le départ Apache, php4 et MySQL.

2ème problème :
Lorsque j'accède à la base de données par l'interface php, j'obtiens un message d'erreur d'accès à la base SQL du type :

Warning: Unable to jump to row 0 on MySQL result index 11 in /var/www/prelude-frontend-php/**index.php** on line 8

Résolution :
Il s'avère que cette erreur est un bug du programme, qui ne permet pas d'accéder aux valeurs de la base si la sonde n'est pas en fonctionnement.

3ème problème :
(ou plutôt inconvénient)
L'interface ne nous donne une liste des alertes, classées par date. Impossibilité de choisir tel ou tel type d'attaque, adresse, port,…
La base devient alors aussi complexe à consulter que le fichier de log en mode texte…

Résolution :
Le module frontend-php ne permet en fait pas plus que lister les alertes. D'après Stéphane Loeuillet (qui a contribué au projet Perl), le concepteur a abandonné l'interface php.
Il faut donc installer le module frontend-perl.

Entre temps n'ayant pas encore eu les réponses aux problèmes, et ayant modifié pas mal de fichiers pour tenter de résoudre ce problème, je décide de repartir sur une base plus saine et de réinstaller le système sous Debian. Cette version de linux étant celle utilisée sur les documentations d'installation trouvées. De plus elle est plus conviviale et permet les installations de librairies plus facilement.

Je réinstalle prelude, et l'interface perl, en suivant les instructions.

4ème problème :
En accédant à l'interface web par l'url :
http://192.168.1.20/piwi/index.pl , j'obtiens une page me demandant un login et un mot de passe. Après avoir essayé différentes possibilités, impossible de se logger.

Résolution :
Cette page par défaut n'est en fait pas nécessaire, mais donne, un exemple de page de présentation et d'authentification.
L'accès peut se faire directement sur la page http://192.168.1.20/piwi/Filters.pl qui est la page d'accès à la liste des alertes.

5ème problème :
Une fois sur l'interface, on a accès à tous les onglets : liste des alertes, classement par date, types d'attaques, adresses sources/dest,…, localisation des adresses, mais aucun onglet pour pouvoir effacer les alertes. Ce problème peut s'avérer assez important, car sur un réseau comme celui du labo, on peut compter sur plus de 100 Mo de données par jour dans la base.

Résolution :
Une des solutions consiste à modifier le fichier /var/www/piwi/Profiles/guest.user afin de lui donner les droits nécessaires pour effacer les alertes.

VI. Conclusion générale

Pourquoi un tel choix de logiciel?
Une stratégie de sécurité est un choix difficile sur plusieurs points:
- Que faut-il sécuriser?
- Contre quoi/qui?
- Avec quels moyens en matériels?
- Avec quels moyens financiers?
Sans compter le fait que, bien souvent, les deux derniers points dépendent des deux premiers.

Il faut donc trouver une solution qui permette de matérialiser les besoins.
Le monde Open source permet de disposer de nombreux logiciels dans plusieurs domaines, et le fait qu'il n'y ai pas besoin d'acquitter des droits de licence, est un choix que l'on peut prendre en compte, car dans une petite entreprise les crédits ne permettent pas toujours de s'offrir des produits payants.

Localement, pour permettre de connaître quels sont les fichiers à protéger, le choix du logiciel est porté sur Tripwire. Léger et simple, il peut permettre de vérifier tout mouvement de fichiers, que l'on aura préalablement sélectionnés. En vérifiant les rapports, on peut établir rapidement un état des lieux sur les données locales sensibles.

Au niveau réseau, la mise en place d'une sonde de détection d'intrusion Prelude, va donner la possibilité de lister toutes les trames à risques qui entre et qui sortent du réseau. Les informations relevées par Prelude, montrent d'où vient le danger, quelles sont les ressources sensibles du domaine.

A mon sens, il y a deux raisons pour mettre en place ce type de logiciels:

Tout d'abord, ils peuvent être installés avant l'achat d'un matériel de protection dédié et/ou payant afin de mieux déterminer les caractéristiques nécessaires et permettront d'opter pour un produit plutôt qu'un autre.

Ensuite, sur un réseau avec une politique de sécurité existante, l'installation de ces moyens d'audit, vient en soutien, et permet de vérifier que la configuration actuelle reste efficace.

ANNEXES

Annexe 1

Exemple de rapport de vérification Tripwire

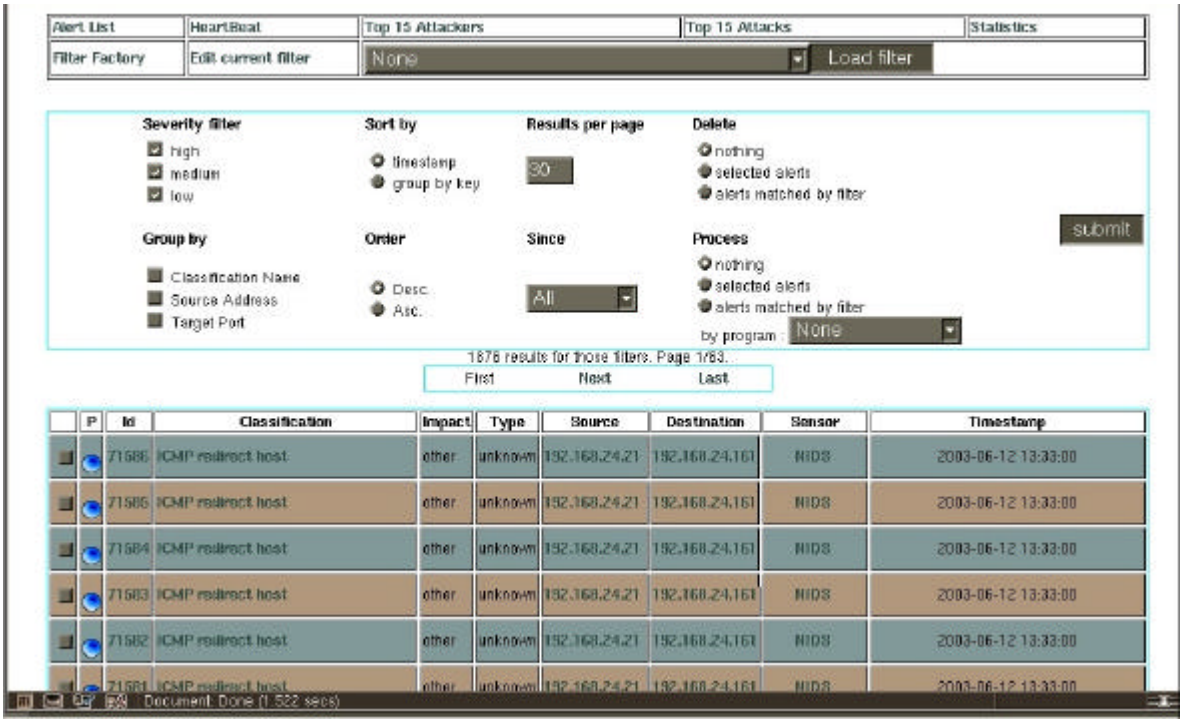
```
Parsing policy file: /etc/tripwire/tw.pol
*** Processing Unix File System ***
Performing integrity check...
Wrote report file: /var/lib/tripwire/report/IDS-20030611-143616.twr


Tripwire(R) 2.3.0 Integrity Check Report

Report generated by:          root
Report created on:            Wed Jun 11 14:36:16 2003
Database last updated on:     Never

===============================================================================
Report Summary:
===============================================================================

Host name:                    IDS
Host IP address:              192.168.24.20
Host ID:                      None
Policy file used:             /etc/tripwire/tw.pol
Configuration file used:      /etc/tripwire/tw.cfg
Database file used:           /var/lib/tripwire/IDS.twd
Command line used:            tripwire --check

===============================================================================
Rule Summary:
===============================================================================

-------------------------------------------------------------------------------
  Section: Unix File System
-------------------------------------------------------------------------------

  Rule Name                       Severity Level    Added    Removed  Modified
  ---------                       --------------    -----    -------  -----
  Invariant Directories           66                0        0        0
  Temporary directories           33                0        0        0
* Tripwire Data Files             100               1        0        0
  Critical devices                100               0        0        0
  User binaries                   66                0        0        0
  Tripwire Binaries               100               0        0        0
  Critical configuration files    100               0        0        0
  Libraries                       66                0        0        0
  Shell Binaries                  100               0        0        0
  File System and Disk Administraton Programs
                                  100               0        0        0
  Kernel Administration Programs  100               0        0        0
  Networking Programs             100               0        0        0
  System Administration Programs  100               0        0        0
  Hardware and Device Control Programs
                                  100               0        0        0
  System Information Programs     100               0        0        0
  Application Information Programs
                                  100               0        0        0
  Shell Releated Programs         100               0        0        0
  Critical Utility Sym-Links      100               0        0        0
  Critical system boot files      100               0        0        0
  System boot changes             100               0        0        0
  OS executables and libraries    100               0        0        0
  Security Control                100               0        0        0
  Login Scripts                   100               0        0        0
```

```
  Operating System Utilities      100             0        0        0
* Root config files               100             0        0        2

Total objects scanned:  8950
Total violations found:  3

===============================================================================
Object Summary:
===============================================================================

-------------------------------------------------------------------------------
# Section: Unix File System
-------------------------------------------------------------------------------

-------------------------------------------------------------------------------
Rule Name: Tripwire Data Files (/var/lib/tripwire)
Severity Level: 100
-------------------------------------------------------------------------------

Added:
"/var/lib/tripwire/IDS.twd"

-------------------------------------------------------------------------------
Rule Name: Root config files (/root)
Severity Level: 100
-------------------------------------------------------------------------------

Modified:
"/root/.kde/share/config"
"/root/.kde/share/config/konquerorrc"

===============================================================================
Error Report:
===============================================================================

No errors

-------------------------------------------------------------------------------
*** End of report ***
```

Annexe 2

Copie d'écran du module Piwi.

Rubrique Alert List

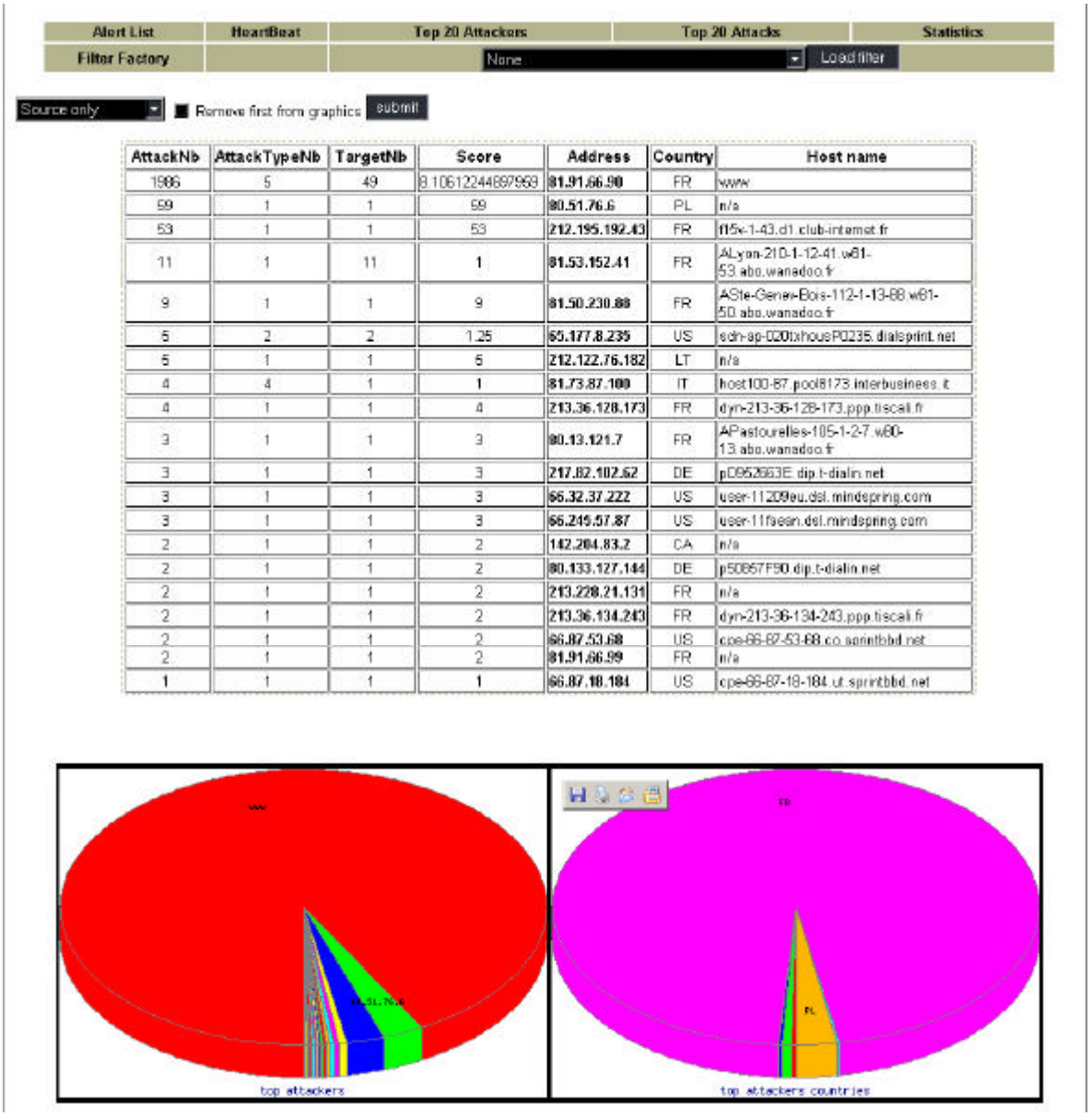


Donne la liste de toutes les alertes enregistrées dans la base.

Rubrique HeartBeat

Fourni les détails sur l'état des capteurs, et permet de voir si il y a eu interruption dans les remontés d'alertes.

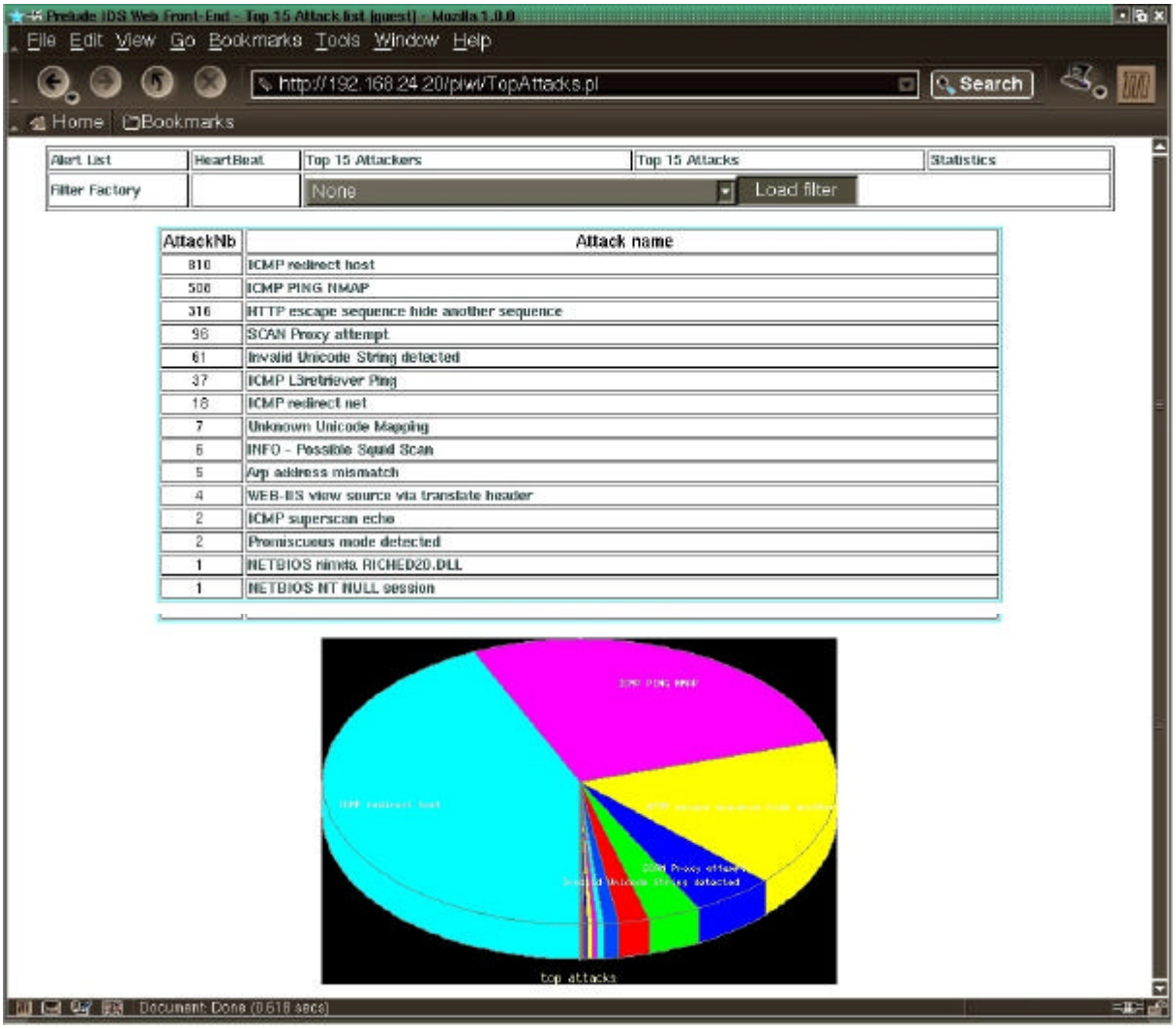
Rubrique Top 15 Attackers



AttackNb	AttackTypeNb	TargetNb	Score	Address	Country	Host name
1986	5	49	8.1061224489796	81.91.66.98	FR	www
59	1	1	59	80.51.76.6	PL	n/a
53	1	1	53	212.195.192.43	FR	f15x-1-43.d1.club-internet.fr
11	1	11	1	81.53.152.41	FR	ALyon-210-1-12-41.w81-53.abo.wanadoo.fr
9	1	1	9	81.50.230.88	FR	ASte-Genev-Bois-112-1-13-88.w81-50.abo.wanadoo.fr
5	2	2	1.25	65.177.8.235	US	sdn-ap-020txhousP0235.dialsprint.net
5	1	1	5	212.122.76.182	LT	n/a
4	4	1	1	81.73.87.100	IT	host100-87.pool8173.interbusiness.it
4	1	1	4	213.36.128.173	FR	dyn-213-36-128-173.ppp.tiscali.fr
3	1	1	3	80.13.121.7	FR	APastourelles-105-1-2-7.w80-13.abo.wanadoo.fr
3	1	1	3	217.82.102.62	DE	p0952663E.dip.t-dialin.net
3	1	1	3	66.32.37.222	US	user-112l9eu.dsl.mindspring.com
3	1	1	3	66.245.57.87	US	user-11faean.dsl.mindspring.com
2	1	1	2	142.204.83.2	CA	n/a
2	1	1	2	80.133.127.144	DE	p50857F90.dip.t-dialin.net
2	1	1	2	213.228.21.131	FR	n/a
2	1	1	2	213.36.134.243	FR	dyn-213-36-134-243.ppp.tiscali.fr
2	1	1	2	66.87.53.68	US	cpe-66-87-53-68.co.sprintbbd.net
2	1	1	2	81.91.66.99	FR	n/a
1	1	1	1	66.87.18.184	US	cpe-66-87-18-184.ut.sprintbbd.net

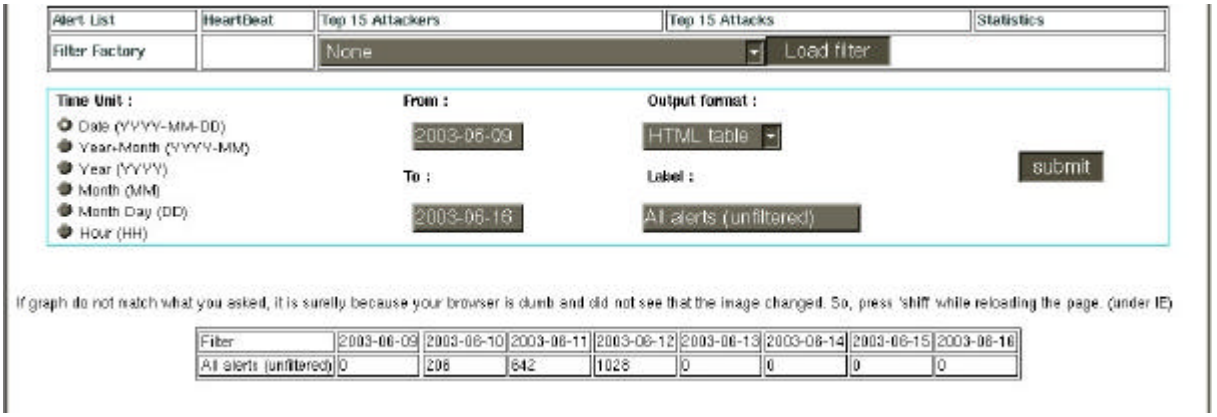
Donne la liste des 15 adresses IP sources les plus fréquentes, avec leur localisation si le module Geo::IP est présent.

Rubrique Top 15 Attacks



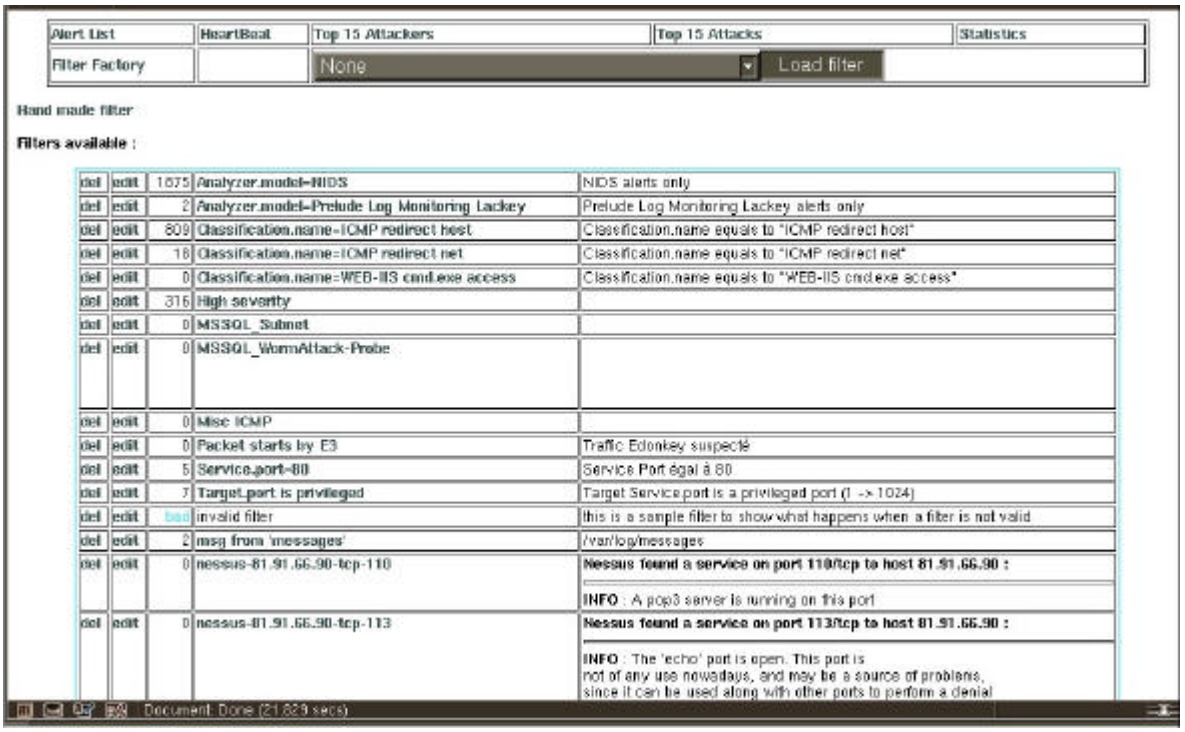
Donne le nombre et le type des 15 alertes les plus fréquentes.

Rubrique Statistics



Statistiques sur les alertes.

Rubrique Filter Factory

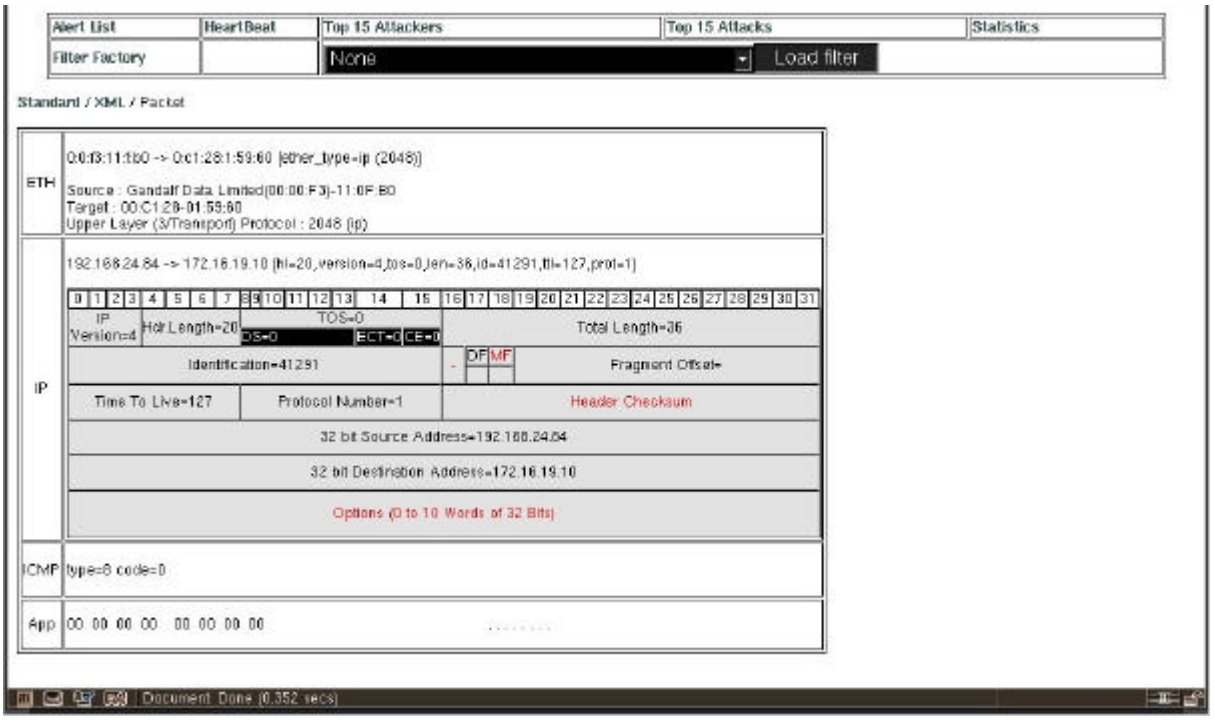

Alert List
HeartBeat
Top 15 Attackers
Top 15 Attacks
Statistics
Filter Factory
None
Load filter
Hand made filter
Filters available :
del edit 1675 Analyzer.model=NIDS NIDS alerts only
del edit 2 Analyzer.model=Prelude Log Monitoring Lackey Prelude Log Monitoring Lackey alerts only
del edit 809 Classification.name=ICMP redirect host Classification.name equals to "ICMP redirect host"
del edit 16 Classification.name=ICMP redirect net Classification.name equals to "ICMP redirect net"
del edit 0 Classification.name=WEB-IIS cmd.exe access Classification.name equals to "WEB-IIS cmd.exe access"
del edit 316 High severity
del edit 0 MSSQL_Subnet
del edit 0 MSSQL_WormAttack-Probe
del edit 0 Misc ICMP
del edit 0 Packet starts by E3 Trafic Edonkey suspecté
del edit 5 Service.port=80 Service Port égal à 80
del edit 7 Target.port is privileged Target Service port is a privileged port (1 -> 1024)
del edit bad invalid filter this is a sample filter to show what happens when a filter is not valid
del edit 2 msg from 'messages' /var/log/messages
del edit 0 nessus-81.91.66.90-tcp-110 Nessus found a service on port 110/tcp to host 81.91.66.90 :
INFO : A pop3 server is running on this port
del edit 0 nessus-81.91.66.90-tcp-113 Nessus found a service on port 113/tcp to host 81.91.66.90 :
INFO : The 'echo' port is open. This port is
not of any use nowadays, and may be a source of problems,
since it can be used along with other ports to perform a denial
Document: Done (21.629 secs)

Cette rubrique permet de lister tous les filtres du modules Perl, pour permettre une séléction plus précise des alertes.

Détails sur une alerte

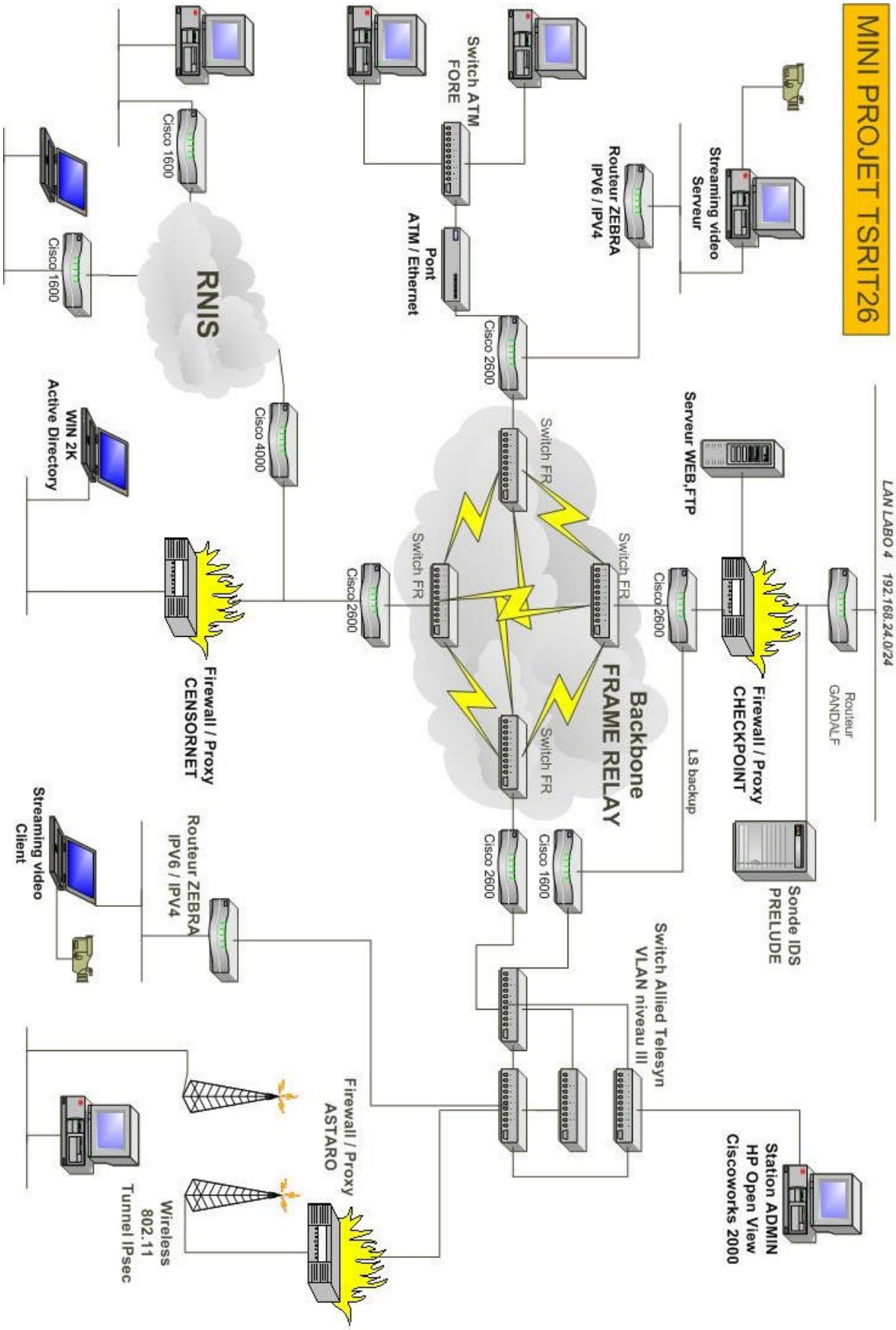
Alert List
HeartBeat
Top 15 Attackers
Top 15 Attacks
Statistics
Filter Factory
None
Load filter
Standard / XML / Packet
Alert #53610 : ICMP superscan echo
Detect time : 2003-06-17 11:26:24 (0xc2997960.0xab30000)
Create time : 2003-06-17 11:26:24 (0xc2997960.0xab34e00)
Classification informations :
Name : ICMP superscan echo
Impact severity :
Description : Attempted Information Leak
Severity : medium
Completion :
Type : recon
Detected by Prelude NIDS (5498904363980899626) :
Analyzer ID : 5498904363980899626
Model : Prelude NIDS
Version : 0.0.1
Manufacturer : The Prelude Team http://www.prelude-ids.org
Class : Network Intrusion Detection System
OS Type : Linux
OS Version : 2.2.20-idepci
Source informations :
Spoofed : unknown
Protocol : unknown
Address type : ipv4-addr
Address : 192.168.24.84
Target informations :
Spoofed :
Protocol : unknown
Address type : ipv4-addr
Address : 172.16.19.10
Additional data :
Snort rule revision : 1
Snort rule ID : 474
Detection Plugin Description : Snort signature parser.
Detection Plugin Contact : prelude-devel@prelude-ids.org
Detection Plugin Author : The Prelude Team
Detection Plugin Name : SnortRules
Payload header : size=8 bytes
Payload Hexadecimal Dump :
00 00 00 00 00 00 00 00
Payload ASCII only Dump :
.....
Icmp header : type=8 code=0
Ip header : 192.168.24.84 -> 172.16.19.10 [hl=20,version=4,tos=0,len=36,id=41291,ttl=127,prot=1]
Ethernet header :
Source : Gandalf Data Limited(00:00:F3):11:0F:80
Target : 00:C1:26:01:58:60
Upper Layer (3/Transport) Protocol : 2048 (ip)

Ici Alerte d'un scan de port, on peut noter la richesse des informations obtenues :
Date, @IP/MAC source, @IP/MAC destination, payload, …



Même alerte avec l'option « Packet ».

Annexe 3


MINI PROJET TSRIT26
LAN LABO 4 192.168.24.0/24
Streaming video Serveur
Switch ATM FORE
Routeur ZEBRA IPV6 / IPV4
Pont ATM / Ethernet
Cisco 2600
Cisco 1600
Cisco 1600
RNIS
Cisco 4000
WIN 2K Active Directory
Serveur WEB,FTP
Switch FR
Switch FR
Switch FR
Switch FR
Backbone FRAME RELAY
Cisco 2600
Cisco 2600
Cisco 2600
Routeur GANDALF
Firewall / Proxy CHECKPOINT
LS backup
Sonde IDS PRELUDE
Firewall / Proxy CENSORNET
Streaming video Client
Routeur ZEBRA IPV6 / IPV4
Cisco 1600
Switch Allied Telesyn VLAN niveau III
Station ADMIN HP Open View Ciscoworks 2000
Firewall / Proxy ASTARO
Wireless 802.11 Tunnel IPsec

Annexe 4

Ressources

Tripwire :

Site officiel
http://www.tripwire.org

Prelude :

Présentation de G. Arcas
http://www.ossir.org/ftp/supports/2002/SUR20020611-GArcas.pdf

Site officiel
http://www.prelude-ids.org/

Anciennes versions
http://www.prelude-ids.org/download/releases/

Interface perl (Prelude-frontend-perl ou Piwi)
http://www.leroutier.net/Projects/

Installation
http://lehmann.free.fr/Prelude.html
2 documents :
- Manuel d'installation et de configuration de PRELUDE (nids / hids / manager / frontend-php / frontend-perl)
- Rapport Final du Travail d'Étude et de Recherche

Présentation, fonctionnement
Magazine M.I.S.C. N°3 (Multi-system & Internet Security Cookbook)

Infos sur les signatures SNORT
http://www.snort.org/snort-db/

Libsafe
http://www.research.avayalabs.com/project/libsafe/

Pour une base de connaissance sur les failles et les parades courantes support papier, je recommande « Hacking Exposed » de S. McClure, J. Scambray, G.Kurtz.